

ENCRYPTION KEY FOR MULTI-KEY ENCRYPTION IN PROGRAMMABLE LOGIC DEVICE

Raymond C. Pang
Stephen M. Trimberger
Jennifer Wong

7 It is sometimes desirable to protect a design used in a PLD from being
8 copied. If the design is stored in a different device from the PLD and read into the
9 PLD through a bitstream, an unencrypted bitstream could be observed and copied
10 as it is being loaded. According to the invention, a bitstream for configuring a
11 PLD with an encrypted design includes unencrypted words for controlling
12 loading of the configuration bitstream and encrypted words that actually specify
13 the design.